Google Cloud VPN Interop Guide

Using Cloud VPN With Fortinet® FortiGate 300C

Contents

Introduction

This guide walks you through the process of configuring the Fortinet 300C for integration with the Google Cloud VPN service. This information is provided as an example only. Please note that this guide is not meant to be a comprehensive overview of IPsec and assumes basic familiarity with the IPsec protocol.

Environment Overview

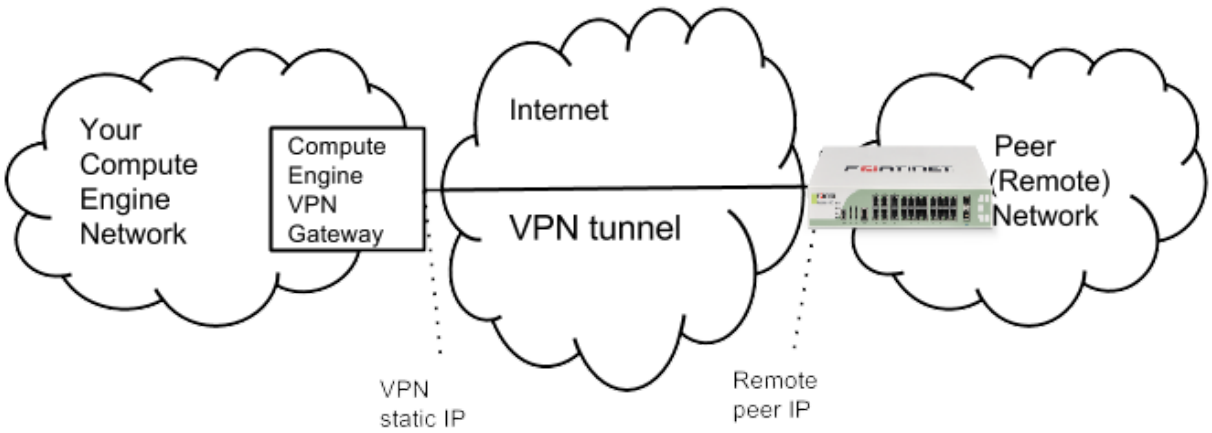
The equipment used in the creation of this guide is as follows:

Vendor:	Fortinet
Model:	FortiGate 300C
Firmware Rev:	04000022
Software Rev:	v5.2.7, build 718 (GA)

Topology

This guide will describe three VPN topologies.

1. A site-to-site policy based IPsec VPN tunnel configuration using static routing
2. A site-to-site route based IPsec VPN tunnel configuration
3. A site-to-site IPsec VPN tunnel configuration using the Google Cloud Router and BGP



Preparation

Overview

The configuration samples which follow will include numerous value substitutions provided for the purposes of example only. Any references to IP addresses, device IDs, shared secrets or keys, account information or project names should be replaced with the appropriate values for your environment when following this guide. Values unique to your environment will be highlighted in **bold**.

This guide is not meant to be a comprehensive setup overview for the device referenced, but rather is only intended to assist in the creation of IPsec connectivity to Google Compute Engine. The following is a high level overview of the configuration process which will be covered:

- Selecting the appropriate IPsec configuration
- Configuring the internet facing interface of your device (outside interface)
- Configuring IKEv2 and IPsec
- Testing the tunnel

Getting Started

The first step in configuring your Fortinet FortiGate for use with the Google cloud VPN service is to ensure that the following prerequisite conditions have been met:

- Fortinet FortiGate online and functional with no faults detected
- Admin access to the Fortinet FortiGate
- At least one configured and verified functional internal interface
- One configured and verified functional external interface

IPsec Parameters

For the Fortinet FortiGate IPsec configuration, the following details will be used:

Parameter	Value
IPsec Mode	ESP+Auth Tunnel mode (Site-to-Site)
Auth Protocol	Pre-shared Key
Key Exchange	IKEv2
Start	auto
Perfect Forward Secrecy (PFS)	on
Dead Peer Detection (DPD)	aggressive
INITIAL_CONTACT (uniqueids)	on

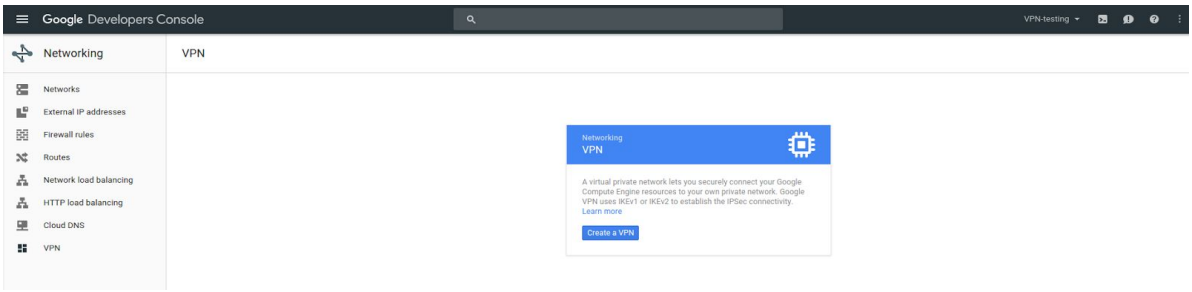
The IPsec configuration used in this guide is specified below:

Phase	*Cipher Role*	*Cipher*
Phase 1	*Encryption*	*aes-256*
	Integrity	*aes256-sha1*
	prf	*sha1-96*
	Diffie-Hellman (DH)	*Group 15*
	Phase 1 lifetime	*36,000 seconds (10 hours)*
Phase 2	*Encryption*	*aes-cbc-256*
	Integrity	*aes256-sha1*

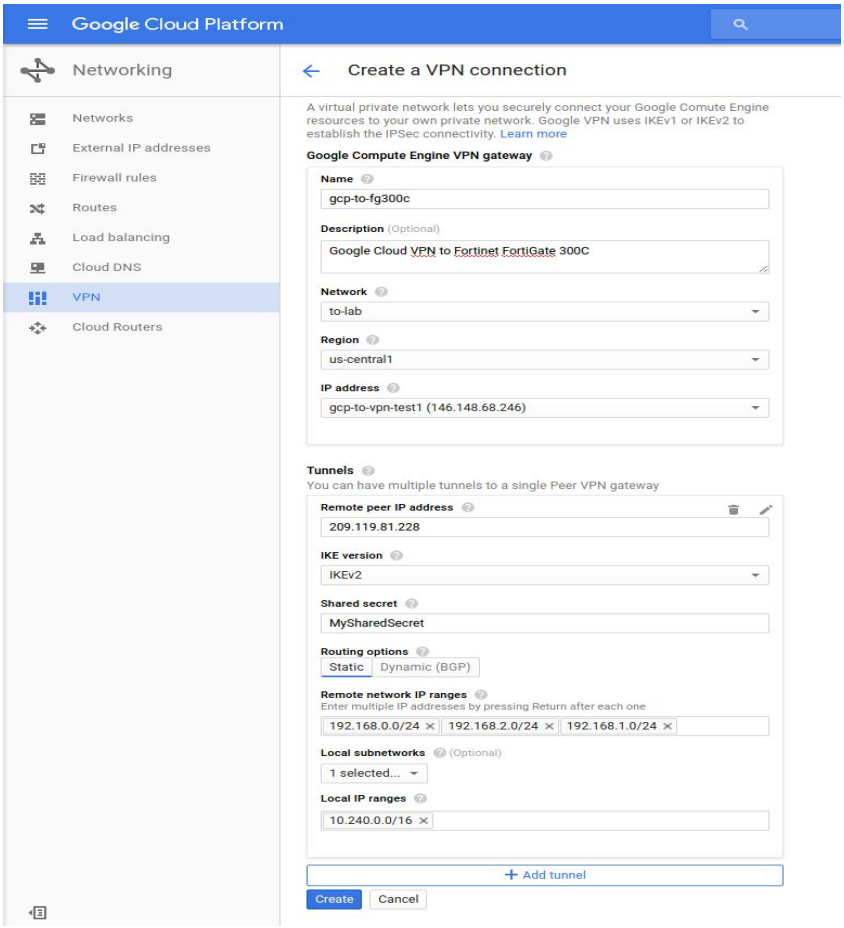
Policy Based IPsec VPN

Configuration - GCP UI

This section provides a step-by-step walkthrough of the Google Cloud Platform VPN configuration. Log on to the Google Cloud Platform Developers Console and select Networking from the main menu. To create a new VPN instance, select the VPN node and click **Create a VPN** from the main task pane:



All parameters needed to create a new VPN connection are entered on this page. A detailed description of each parameter is provided below:



The following parameters are required for the VPN gateway:

- **Name:** the name of the VPN gateway.
- **Description:** a brief description of the VPN connection.
- **Network:** the GCP network the VPN gateway will attach to. **Note:** this is the network to which VPN connectivity will be made available.
- **Region:** the home region of the VPN gateway. **Note:** the VPN gateway must be in the same region as the subnetworks it is connecting.
- **IP address:** the static public IP address which will be used by the VPN gateway. An existing, unused, static public IP address within the project can be assigned, or a new one can be created.

The following parameters are required for each Tunnel which will be managed by the VPN gateway:

- **Remote peer IP address:** the public IP address of the on premises VPN appliance which will be used to connect to Cloud VPN.
- **IKE version:** the IKE protocol version. This guide assumes **IKEv2**
- **Shared secret:** a shared secret used for mutual authentication by the VPN gateways. The on-premises VPN gateway tunnel entry should be configured it the same shared secret.
- **Routing options:** Cloud VPN supports multiple routing options for the exchange of route information between the VPN gateways. For this example **static routing** is being used. Cloud Router and BGP are covered later in this guide.
- **Remote network IP ranges:** the on-premises CIDR blocks being connected to GCP via the VPN gateway.
- **Local subnetworks:** the GCP CIDR blocks being connected to on-premises via the VPN gateway.
- **Local IP ranges:** the GCP IP ranges matching the selected subnet

Configuration - GCP CLI

Cloud VPN can also be configured using the gcloud command line tool. Command line configuration requires two steps. First the VPN Gateway is created, then the tunnels are created referring to the VPN Gateway.

Create the VPN Gateway

```
gcloud compute target-vpn-gateways create gcp-to-fg300c --network to-lab --region
us-central1
```

Create the VPN Tunnel

```
gcloud compute vpn-tunnels create my-tunnel --shared-secret MySharedSecret
--peer-address on-prem-IP --target-vpn-gateway gcp-to-fg300c
--local-traffic-selector gcp-CIDR --remote-traffic-selector on-prem-CIDR
```

Configuration - Fortinet FortiGate 300C: CLI

IPsec Configuration

Create the Phase 1 Configuration

```
config vpn ipsec phase1-interface
    edit "GCP"
        set interface "port1"
        set ike-version 2
        set keylife 36000
        set proposal aes256-sha1
        set comments "VPN: GCP (Created by VPN wizard)"
        set dhgrp 15
        set remote-gw 146.148.68.246
        set psksecret ENC
wDfCX7ikIVbjhh9+DAaX0rCO8x/gnuaFu/yl/flQKuh0SLUURBbG7ITM7MQ+y6TG3ZzUxNWIRlruDPZlgNcqCi
/VEEk5S/vx0DHI81UCBkNz0i1JK7rRdlCQoMepvw+hSU79BlfIPAI2oi7xt+6a6uGYPB3Eszweeqw/YCYQtfyE
+fPGl1NQYcMbkXpa5tBeN6VTLg==
    next
end
```

Create the Phase 2 Configuration

```
config vpn ipsec phase2-interface
    edit "Lab_1"
        set phase1name "GCP"
        set proposal aes256-sha1
        set dhgrp 15
        set replay enable
        set keylifeseconds 10800
        set src-subnet 192.168.1.0 255.255.255.0
        set dst-subnet 10.240.0.0 255.255.0.0
    next
    edit "Lab_0"
        set phase1name "GCP"
        set proposal aes256-sha1
        set dhgrp 15
        set replay enable
        set keylifeseconds 10800
        set src-subnet 192.168.0.0 255.255.255.0
        set dst-subnet 10.240.0.0 255.255.0.0
    next
    edit "Lab_2"
        set phase1name "GCP"
        set proposal aes256-sha1
        set dhgrp 15
```

```
        set replay enable
        set keylifeseconds 10800
        set src-subnet 192.168.2.0 255.255.255.0
        set dst-subnet 10.240.0.0 255.255.0.0
    next
end
```

Firewall Policy

Create the Address Objects

For **remote** subnet entries, substitute the Google Cloud Platform network subnet. For **local** subnet entries, substitute the local 300C subnets:

```
config firewall address
    edit "GCP_remote_subnet_1"
        set uuid 97d79d28-0d99-51e6-8561-1a312ce9ba71
        set subnet 10.240.0.0 255.255.0.0
    next
    edit "GCP_local_subnet_2"
        set uuid 97987828-0d99-51e6-3690-6c658de88669
        set subnet 192.168.2.0 255.255.255.0
    next
    edit "GCP_local_subnet_1"
        set uuid e989f17c-0da6-51e6-1722-80cb52bd4c01
        set subnet 192.168.1.0 255.255.255.0
    next
    edit "GCP_local_subnet_0"
        set uuid f5a5ab0e-0da6-51e6-098d-30320f324a0c
        set subnet 192.168.0.0 255.255.255.0
    next
end
```

Create the Address Groups

Create groups for the **local** and **remote** address objects created above:

```
config firewall addrgrp
    edit "GCP_local"
        set uuid 979d18b0-0d99-51e6-d282-83ea3a020898
        set member "GCP_local_subnet_2" "GCP_local_subnet_0" "GCP_local_subnet_1"
        set comment "VPN: GCP (Created by VPN wizard)"
    next
    edit "GCP_remote"
        set uuid 97dc53a4-0d99-51e6-4728-b7b8405649e1
        set member "GCP_remote_subnet_1"
        set comment "VPN: GCP (Created by VPN wizard)"
    next
End
```

Create the Firewall Policies

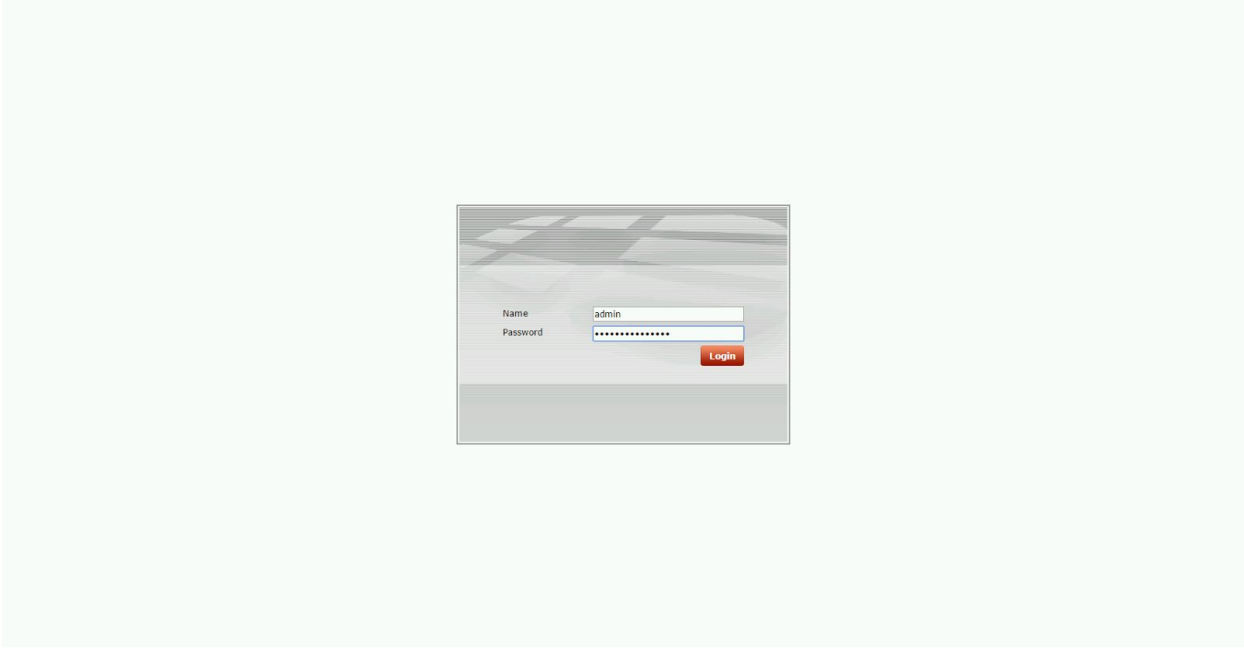
Create two firewall policies, one for Google Cloud Platform network ingress to the 300C local subnets, and one for 300C local subnet egress to the Google Cloud Platform network:

```
config firewall policy
    edit 3
        set uuid 97df898e-0d99-51e6-ff7b-2e266549c953
        set srcintf "port2"
        set dstintf "GCP"
        set srcaddr "GCP_local"
        set dstaddr "GCP_remote"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set comments "VPN: GCP (Created by VPN wizard)"
    next
    edit 4
        set uuid 97e2f15a-0d99-51e6-b260-bbe2fc82b4bf
        set srcintf "GCP"
        set dstintf "port2"
        set srcaddr "GCP_remote"
        set dstaddr "GCP_local"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set comments "VPN: GCP (Created by VPN wizard)"
    next
end
```

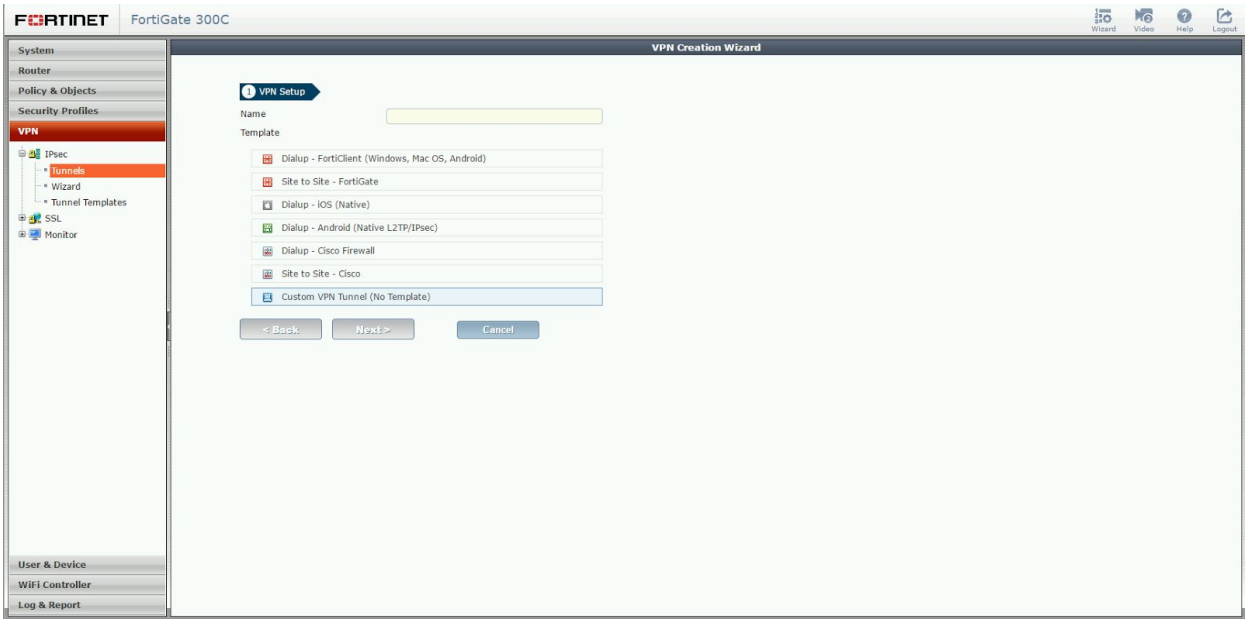
Configuration - Fortinet FortiGate 300C: GUI

IPsec Configuration

Login to the Fortinet device using a web browser:



From the VPN configuration option, choose Tunnels to set up a new VPN connection and select “Custom VPN Tunnel (No Template)” from the wizard:



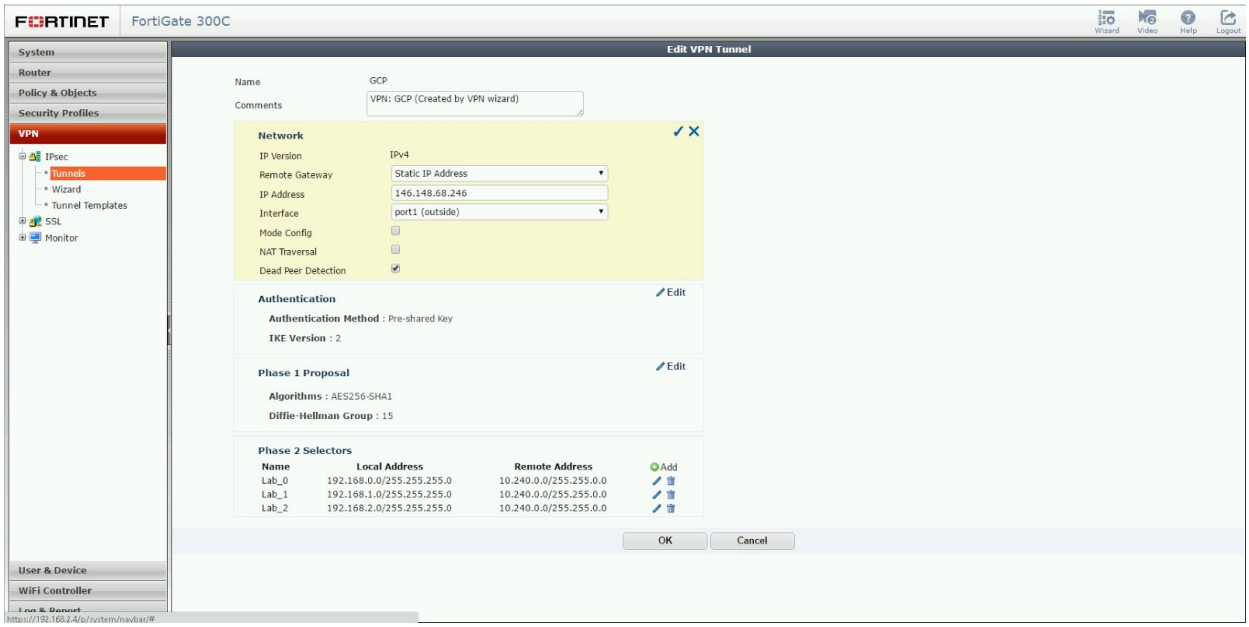
Populate the VPN Tunnel configuration **Network** section as pictured below:

Remote Gateway: select “Static IP Address”

IP Address: enter the IP address of the Google Cloud VPN Gateway

Interface: select the **public** interface of the Fortinet device

Dead Peer Detection: select this checkbox to enable DPD

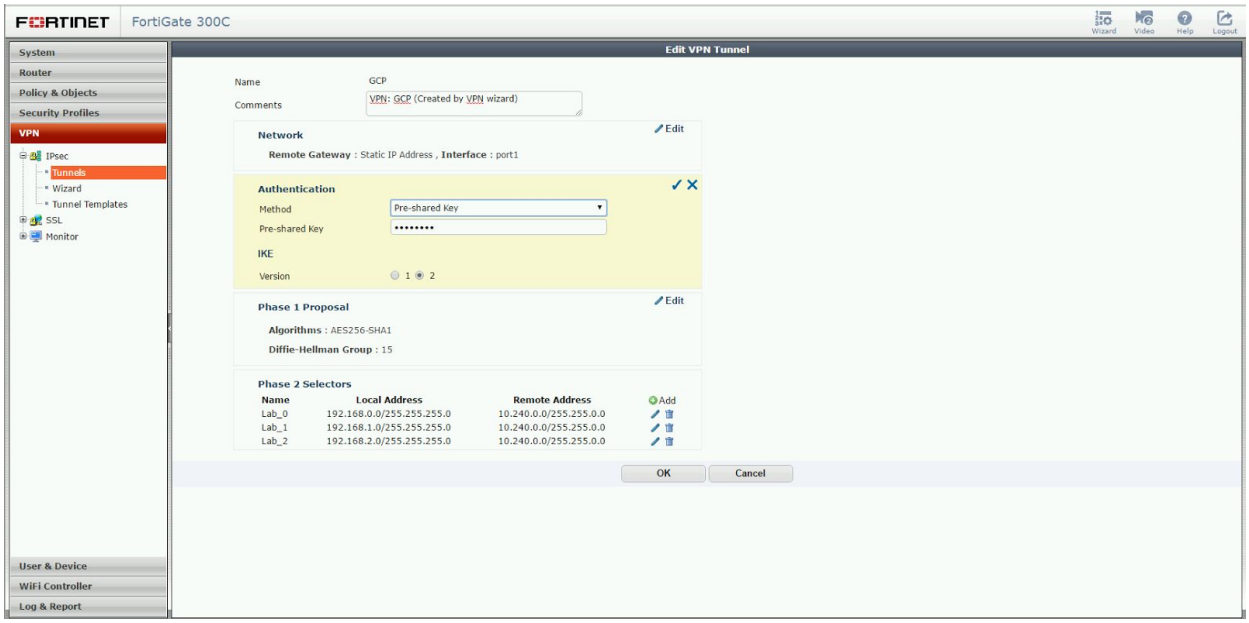


Populate the VPN Tunnel configuration **Authentication** section as pictured below:

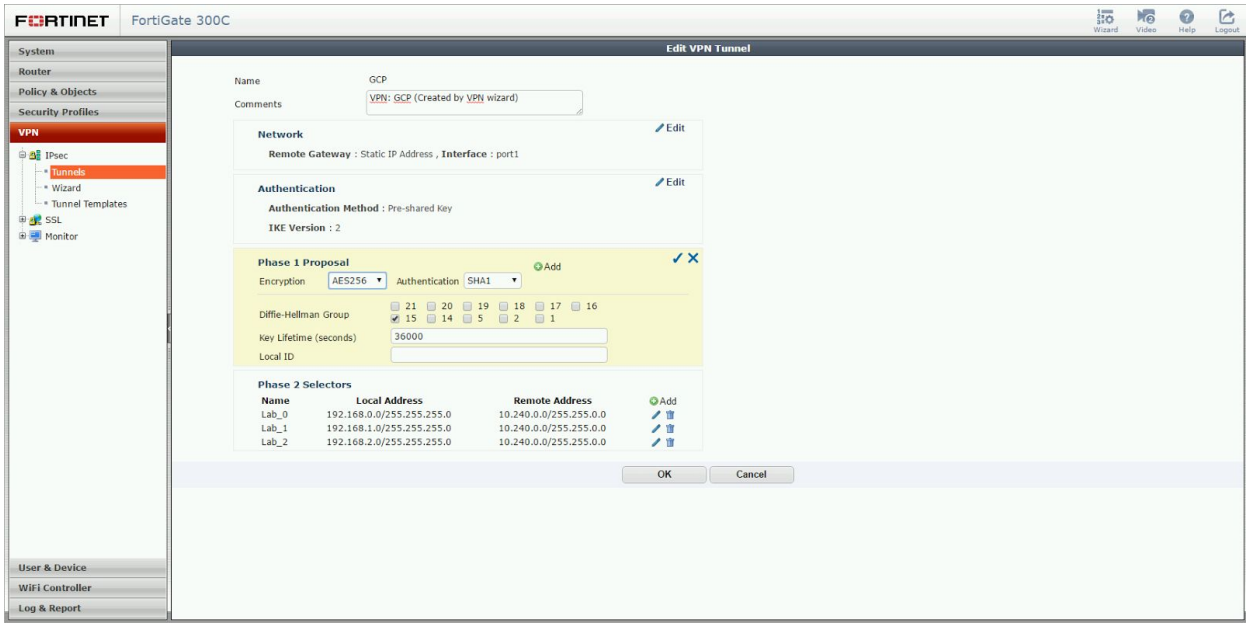
Method: for the authentication method select “Pre-Shared Key”

Pre-Shared-Key: enter the pre-shared key you have chosen to use

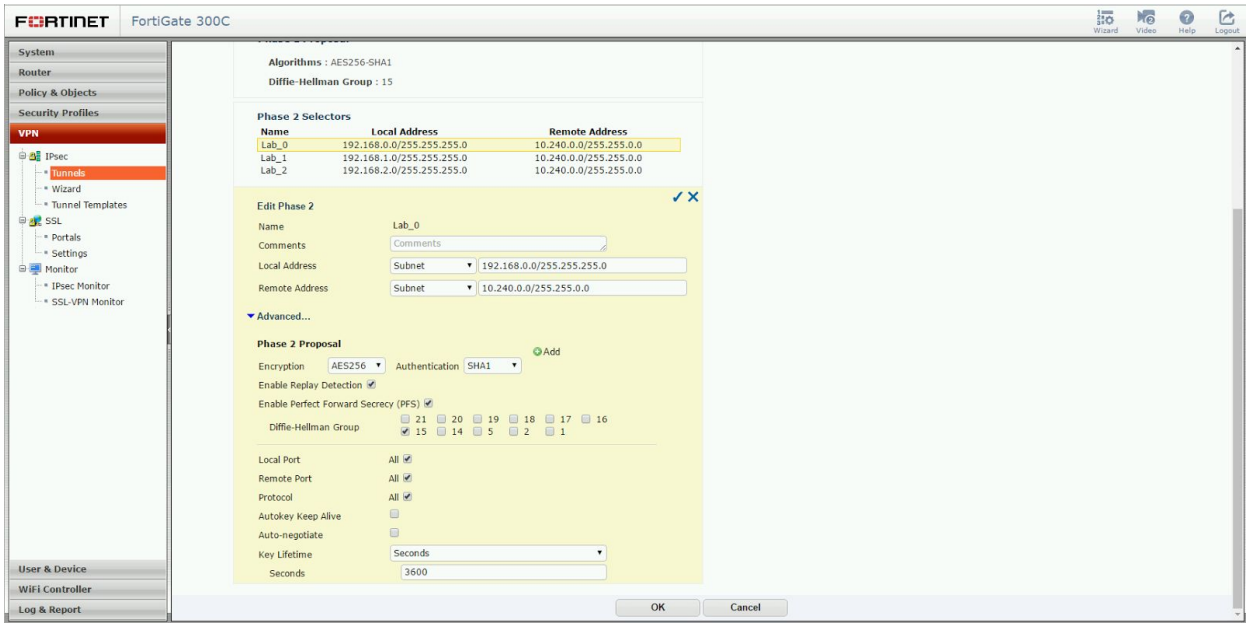
IKE: select IKE version 2



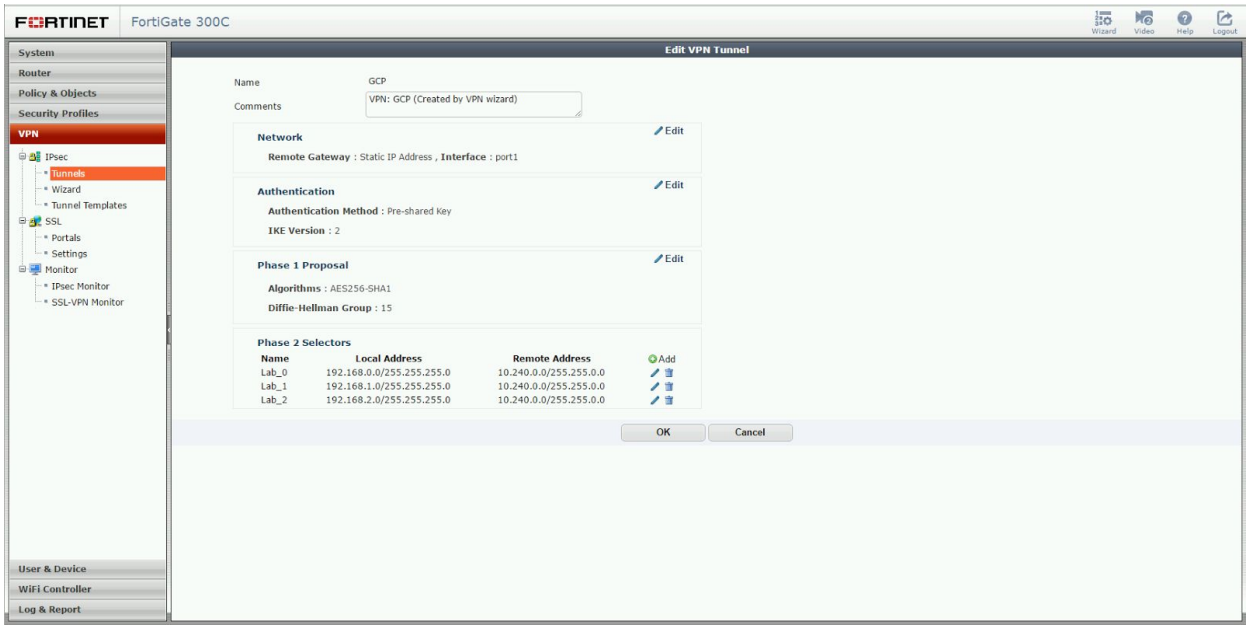
Populate the VPN Tunnel configuration **Phase 1 Proposal** section as pictured below:



Populate the VPN Tunnel configuration **Phase 2 Proposal** section as pictured below:

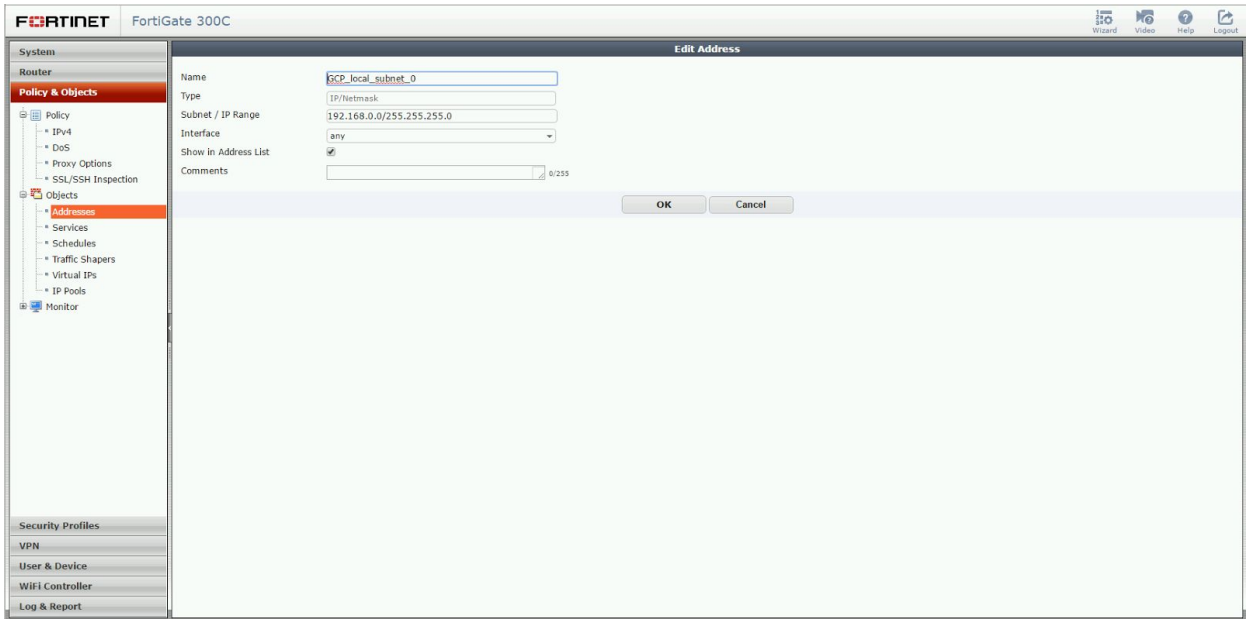


The completed tunnel configuration will appear as below:

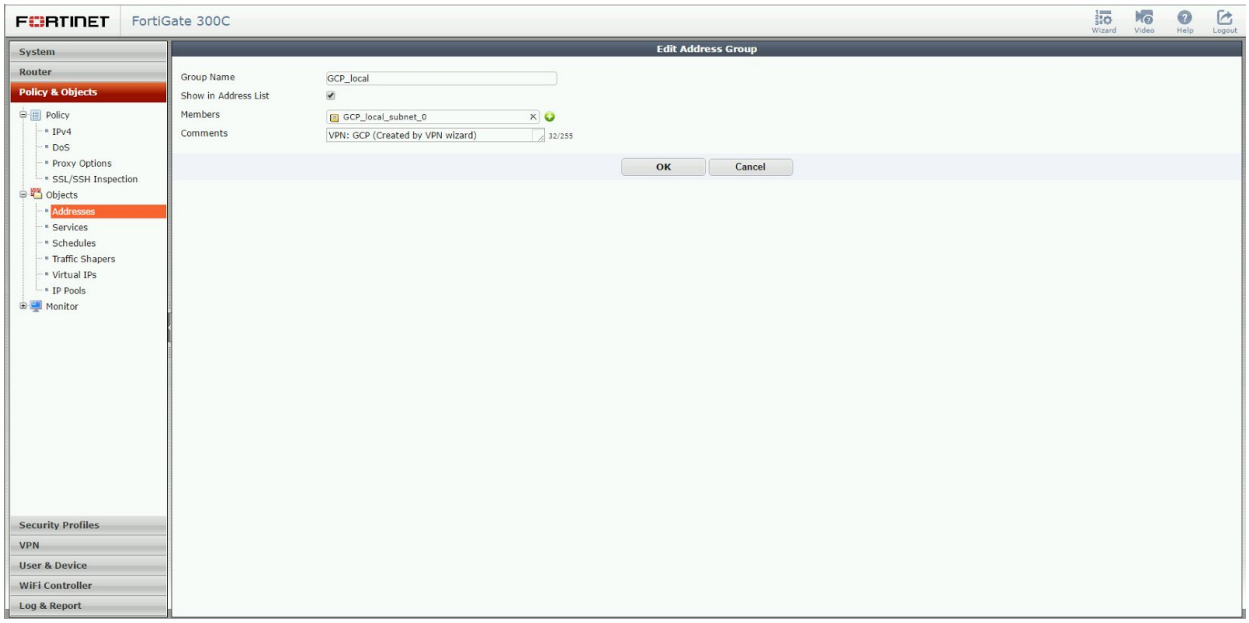


Firewall Policy

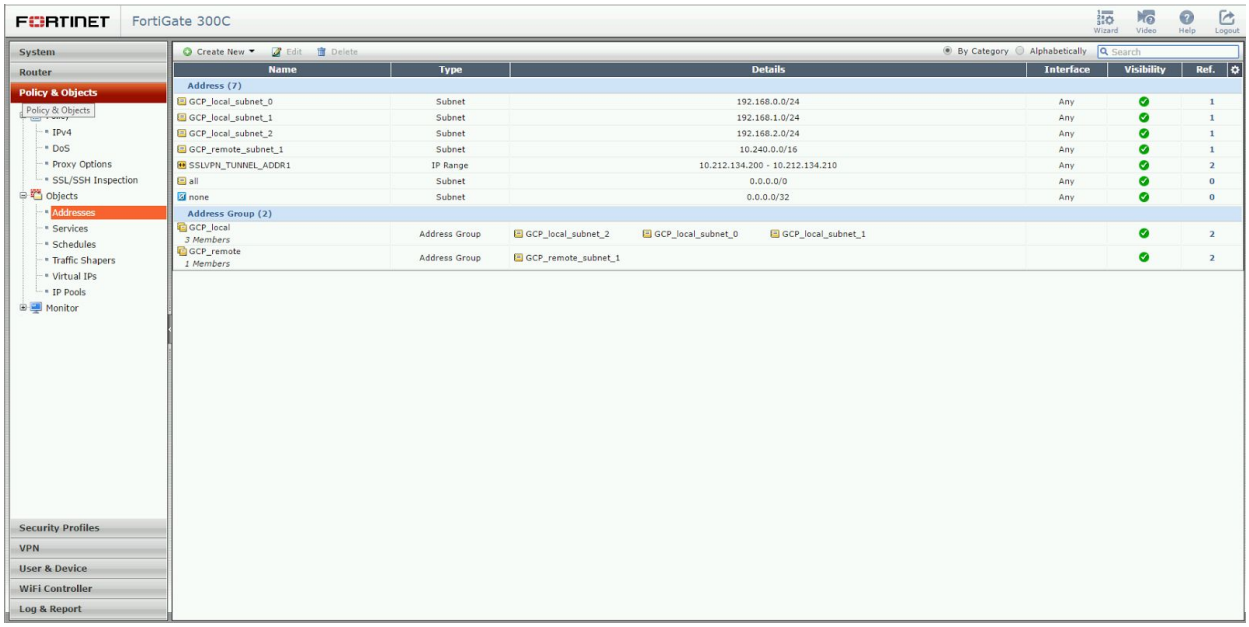
First, from the **Policy & Objects** configuration section, under **Objects**, select **Addresses** and create a new **Address** entry for each subnet (local subnets and remote GCP subnets):



Add all **Address** entries to the appropriate **Address Group** where the entries representing local subnets are added to a local group, and the entries representing GCP subnets (remote) are added to a remote group:

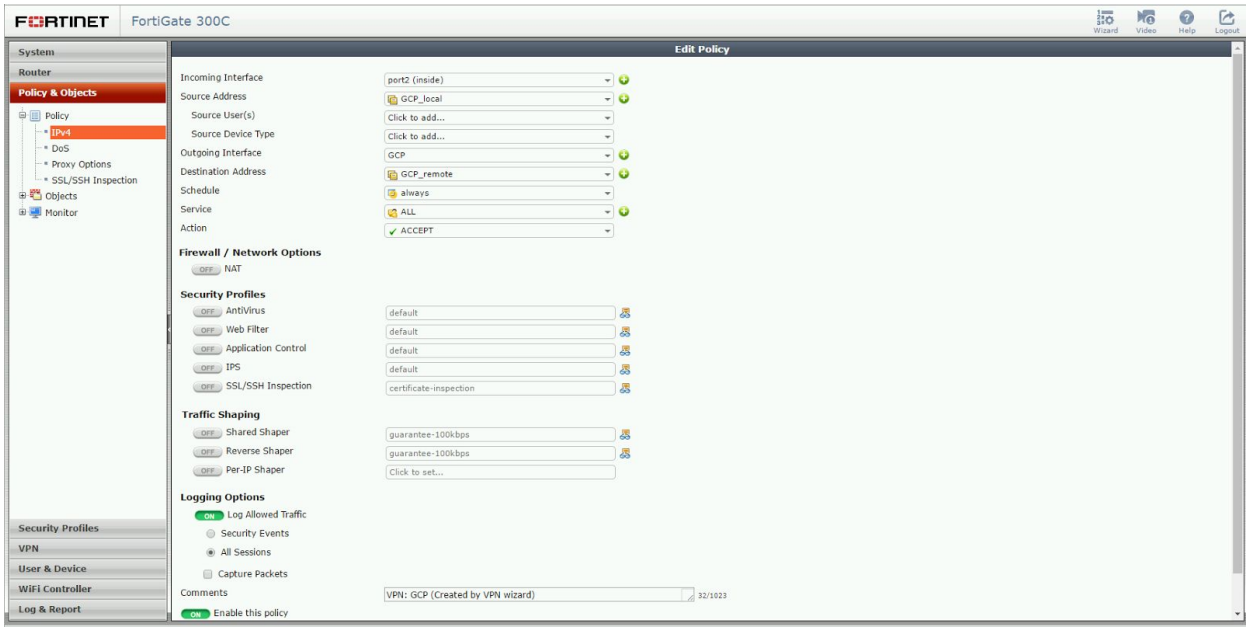


The completed **Addresses** configuration will appear as below:

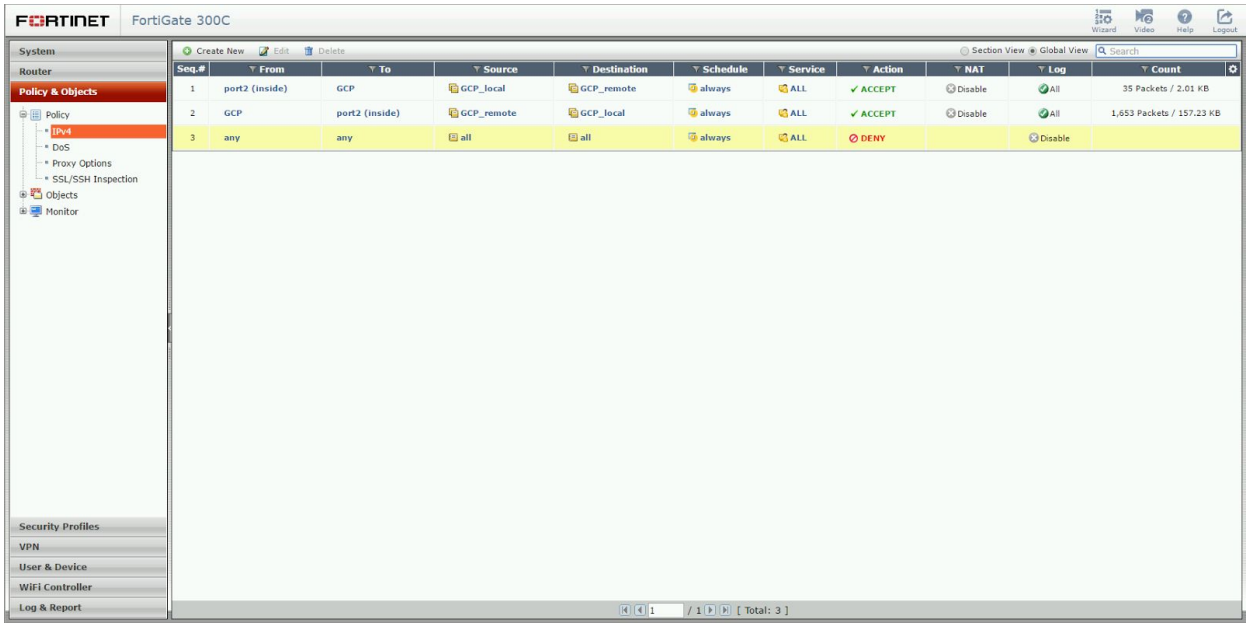


Next, from the **Policy & Objects** configuration section, under **Policy**, select **IPv4** and create new firewall **Policy** entries for ingress and egress:

Incoming Interface: originating interface (inside for egress, outside for ingress)
Source Address: address group created in the prior section (local or remote)
Outgoing Interface: exit interface (inside for egress, outside for ingress)
Destination Address: address group created in the prior section (local or remote)
Schedule: Always (or limit if required)
Service: All (or limit if required)
Action: ACCEPT



After completion there should be two policies, one for ingress and one for egress:



Route Based IPsec VPN

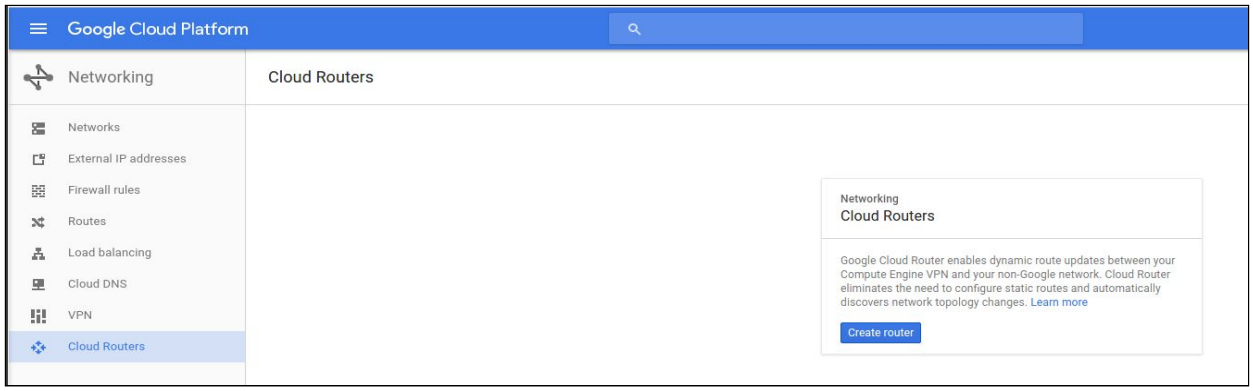
IPsec VPN Using Cloud Router

Configuration - Google Cloud Router UI

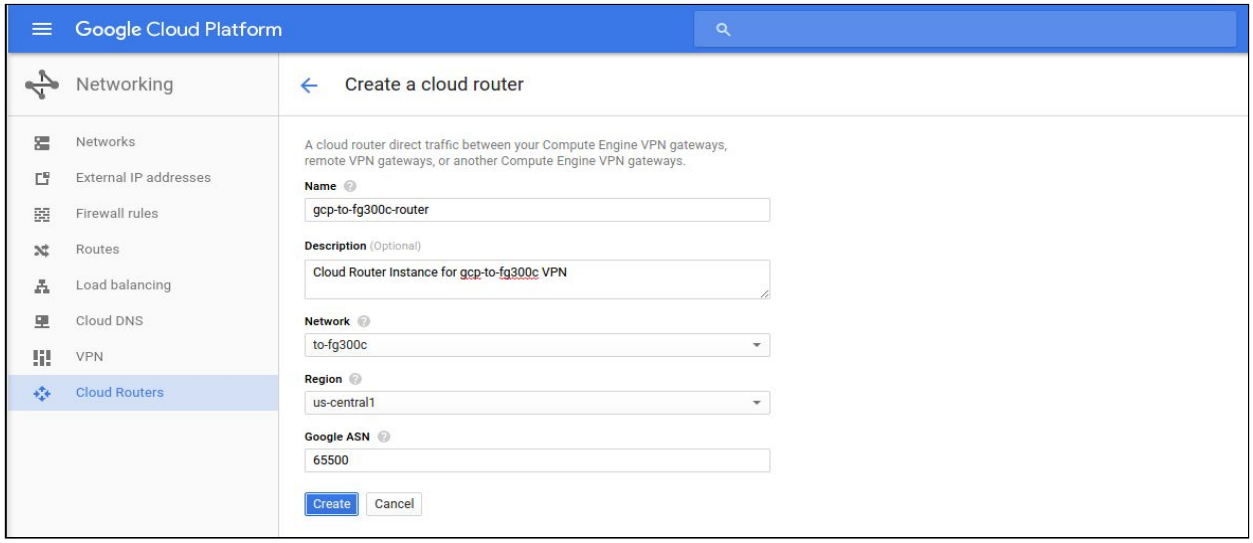
Google Cloud Router enables dynamic Border Gateway Protocol (BGP) route updates between your Google Cloud Platform network and your on-premise network. For the initial release, Cloud Router supports BGP for Cloud VPN only. Cloud Router works with both legacy networks and Subnetworks.

Cloud Router

The first step in configuring the Google Cloud Platform for site-to-site VPN connectivity utilizing BGP and the Google Cloud Router is to create a new cloud router. From the Developer Console, select **Networking** and then **Cloud Routers**. From the workspace select **Create Router**:

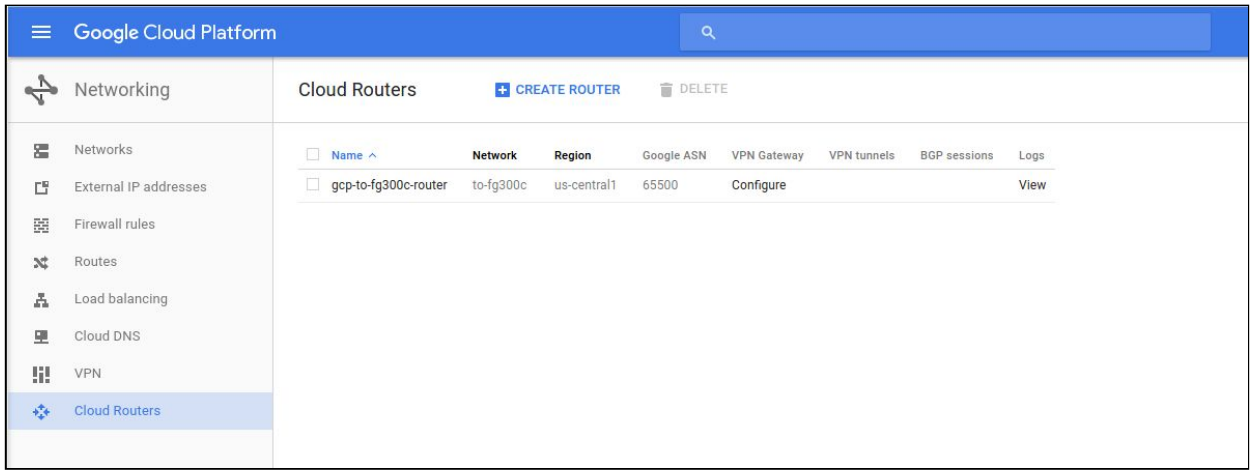


All parameters needed to create a new cloud router are entered on this page. A detailed description of each parameter is provided below:



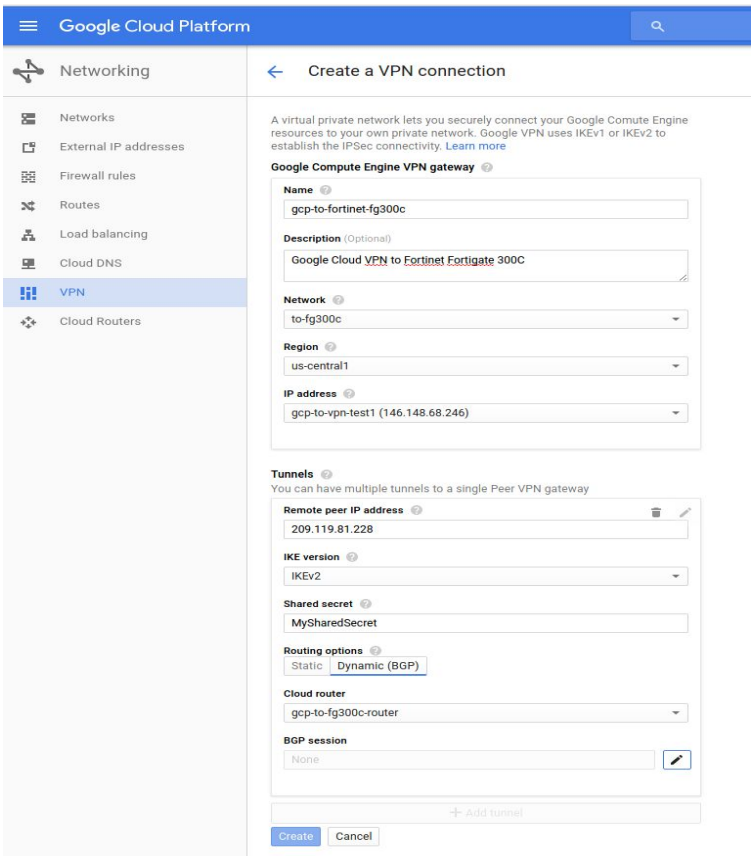
- **Name:** the name of the cloud router.
- **Description:** a brief description of the cloud router.
- **Network:** the GCP network the cloud router will attach to. **Note:** this is the network on route information will be managed.
- **Region:** the home region of the cloud router. **Note:** the cloud router must be in the same region as the subnetworks it is connecting.
- **Google ASN**: the BGP Autonomous System Number assigned to the cloud router. Use any private ASN (64512 - 65534, 4200000000 - 4294967294) not in use elsewhere in the network

The newly created instance will appear in the list of Cloud Routers. Click **Configure** under VPN Gateway to create the VPN tunnel:



VPN Tunnel

All parameters needed to create a new VPN connection are entered on this page. A detailed description of each parameter is provided below:



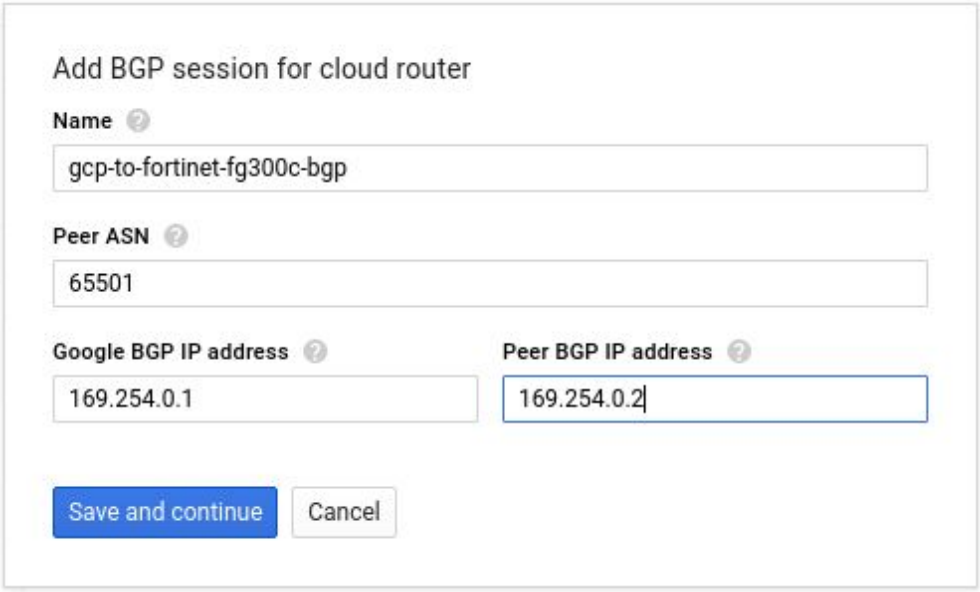
The following parameters are required for the VPN gateway:

- **Name:** the name of the VPN gateway.
- **Description:** a brief description of the VPN connection.
- **Network:** the GCP network the VPN gateway will attach to. **Note:** this is the network to which VPN connectivity will be made available.
- **Region:** the home region of the VPN gateway. **Note:** the VPN gateway must be in the same region as the subnetworks it is connecting.
- **IP address:** the static public IP address which will be used by the VPN gateway. An existing, unused, static public IP address within the project can be assigned, or a new one can be created.

The following parameters are required for each Tunnel which will be managed by the VPN gateway:

- **Remote peer IP address:** the public IP address of the on premises VPN appliance which will be used to connect to Cloud VPN.

- **IKE version:** the IKE protocol version. This guide assumes **IKEv2**
- **Shared secret:** a shared secret used for mutual authentication by the VPN gateways. The on-premises VPN gateway tunnel entry should be configured it the same shared secret.
- **Routing options:** Cloud VPN supports multiple routing options for the exchange of route information between the VPN gateways. For this example **Dynamic (BGP)** is being used. Static Routes were covered earlier in this guide.
- **Cloud Router:** the Cloud Router instance associated with this VPN tunnel created in the Cloud Router section.
- **BGP session:** the BGP configuration to be used by the Cloud Router for this VPN tunnel. Click the pencil to create a new configuration:



The following parameters are required to configure the BGP session:

- **Name:** the name of the BGP session
- **Peer ASN:** the unique BGP ASN of the on-premises router
- **Google BGP IP address, Peer BGP IP address:** The Google BGP IP and Peer BGP IP must be link-local in the same /30 subnet. Make sure they aren't the network or broadcast address of the subnet.

Once all of the BGP session info has been entered, click **Save and continue** to complete, then click **Create** on the Create a VPN connection form to create the VPN connection.

Configuration - Google Cloud Router CLI

Cloud VPN can also be configured using the gcloud command line tool. Command line configuration requires multiple steps.

Create the VPN Gateway

Create the VPN gateway. Make note of the chosen name (**my-gateway**), network and region for use in future steps:

```
gcloud compute target-vpn-gateways create my-gateway --project my-project --network
my-network --region my-region
```

Reserve a Static IP

Reserve a static IP address in the Google Cloud Platform network and region where the VPN gateway was created. Make a note of the created address for use in future steps.

```
gcloud compute addresses create vpn-static-ip --project my-project --region my-region
```

Create the Cloud Router

Create a Cloud Router in the region where the VPN gateway was created. This example uses ASN 65001 for the Cloud Router ASN, but any private ASN (64512 - 65534, 4200000000 - 4294967294) not already in use in the peer network can be used:

```
gcloud beta compute --project my-project routers create my-router --region my-region
--network my-network --asn my-asn
```

Create the VPN Tunnel

Create the VPN tunnel referencing the **VPN gateway** and **Cloud Router** created earlier. Make note of the chosen tunnel name for use in future steps. The **peer-address** should be set to the outside interface IP of the Fortinet device and a **shared-secret** should be set which will be used later in configuring the Fortinet side of the tunnel.

```
gcloud beta compute --project my-project vpn-tunnels create my-tunnel --region
my-region --ike-version 2 --target-vpn-gateway my-gateway  --peer-address my-IP
--shared-secret my-PSK --router my-router
```

Add the BGP Link Local Interface

Update the Cloud Router config to add a virtual interface (--interface-name) for the BGP peer. The BGP interface IP address must be a link-local IP address belonging to the IP address range 169.254.0.0/16 and it must belong to same subnet as the interface address of the peer router.

The netmask length is recommended to be 30. Make sure each tunnel has a unique pair of IPs. Alternatively, if --ip-address and --mask-length are blank, and --peer-ip-address in the next step is left blank, the IP addresses will be automatically generated:

```
gcloud beta compute --project my-project routers add-interface my-router
--interface-name my-if --ip-address my-link-local-IP --mask-length 30 --vpn-tunnel
my-tunnel --region my-region
```

Add the BGP Peering Session

Update the Cloud Router config to add the BGP peer to the interface. This example uses ASN 65002 for the peer ASN. Any public ASN or private ASN (64512 - 65534, 4200000000 - 4294967294) not already in use in the peer network can be used. The BGP peer interface IP address must be a link-local IP address belonging to the IP address range 169.254.0.0/16. It must belong to same subnet as the Google Cloud Platform-side interface. Make sure each tunnel has a unique pair of IPs.

```
gcloud beta compute --project my-project routers add-bgp-peer my-router --peer-name
bgp-peer1 --interface-name my-if --peer-ip-address my-link-local-IP --peer-asn my-ASN
--region my-region
```

Configuration - Fortinet FortiGate 300C: CLI

Interface Configuration

Configure the Tunnel Interface

```
config system interface
 edit "GCP"
        set vdom "root"
        set ip 169.254.0.2 255.255.255.255
        set type tunnel
        set remote-ip 169.254.0.1
        set snmp-index 15
        set interface "port1"
 next
End
```

IPsec Configuration

Create the Phase 1 Configuration

```
config vpn ipsec phase1-interface
    edit "GCP"
        set interface "port1"
        set ike-version 2
        set nattraversal disable
        set keylife 36000
        set proposal aes256-sha1
        set comments "VPN: GCP (Created by VPN wizard)"
        set dhgrp 15
        set remote-gw 146.148.68.246
        set psksecret ENC
wDfCX7ikIVbjhh9+DAaX0rCO8x/gnuaFu/yl/flQKuh0SLUURBbG7ITM7MQ+y6TG3ZzUxNWIRlruDPZlgNcqCi/VEEk5S/
vx0DHI81UCBkNz0i1JK7rRdlCQoMepvw+hSU79BlfIPAI2oi7xt+6a6uGYPB3Eszweeqw/YCYQtfyE+fPGl1NQYcMbkXpa
5tBeN6VTLg==
    next
end
```

Create the Phase 2 Configuration

```
config vpn ipsec phase2-interface
    edit "Lab_2"
        set phase1name "GCP"
        set proposal aes256-sha1
        set dhgrp 15
       set replay enable
        set keylifeseconds 10800
    next
end
```

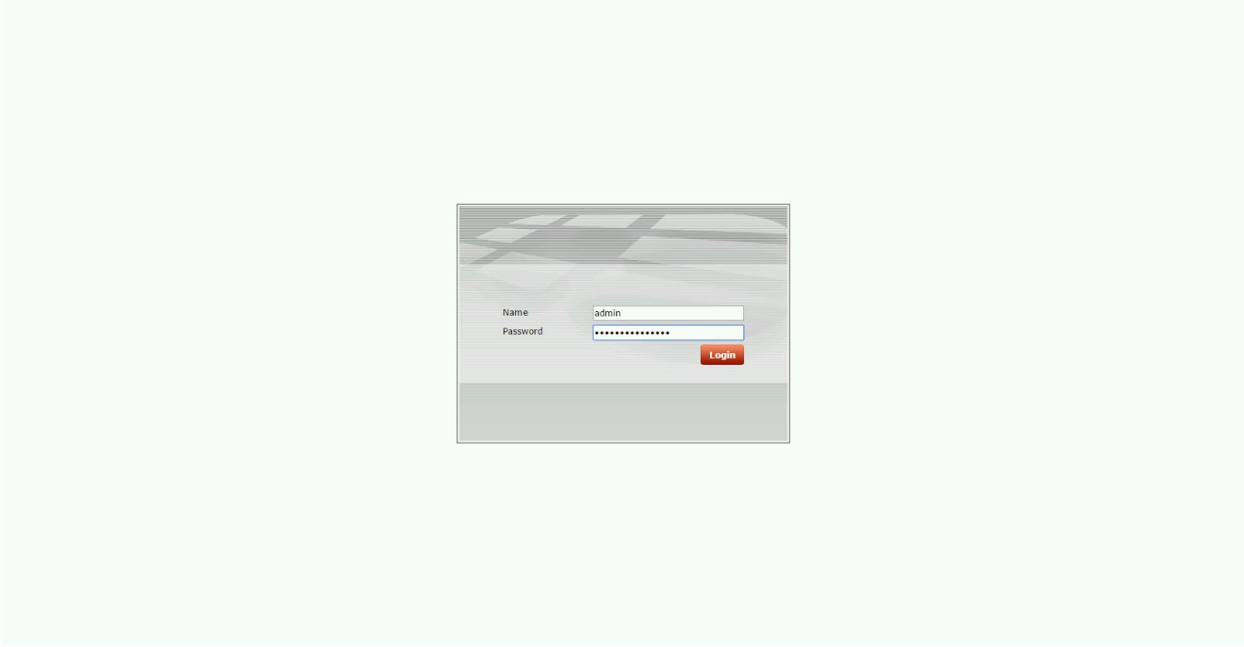
Configure BGP Routing

```
config router bgp
    set as 65501
    set router-id 169.254.0.2
        config neighbor
            edit "169.254.0.1"
                set remote-as 65500
                set send-community6 disable
            next
        end
        config redistribute "connected"
            set status enable
        end
        config redistribute "rip"
        end
        config redistribute "ospf"
        end
        config redistribute "static"
            set status enable
        end
        config redistribute "isis"
        end
        config redistribute6 "connected"
        end
        config redistribute6 "rip"
        end
        config redistribute6 "ospf"
        end
        config redistribute6 "static"
        end
        config redistribute6 "isis"
        end
end
```

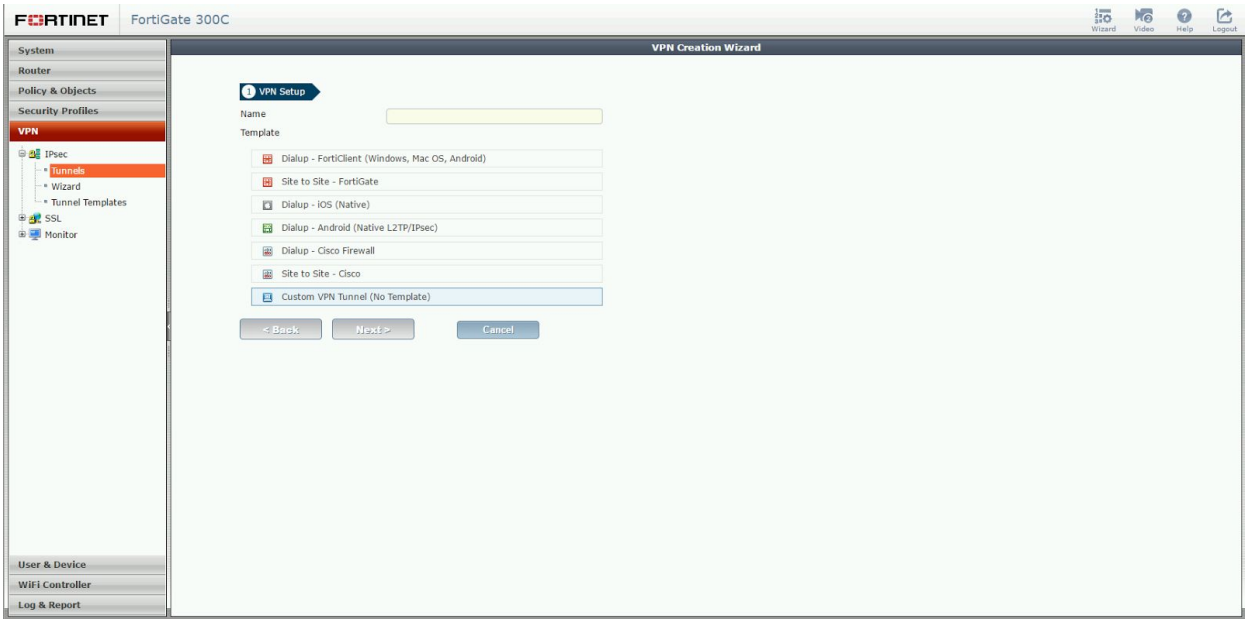
Configuration - Fortinet FortiGate 300C: GUI

IPsec Configuration

Login to the Fortinet device using a web browser:



From the VPN configuration option, choose Tunnels to set up a new VPN connection and select “Custom VPN Tunnel (No Template)” from the wizard:



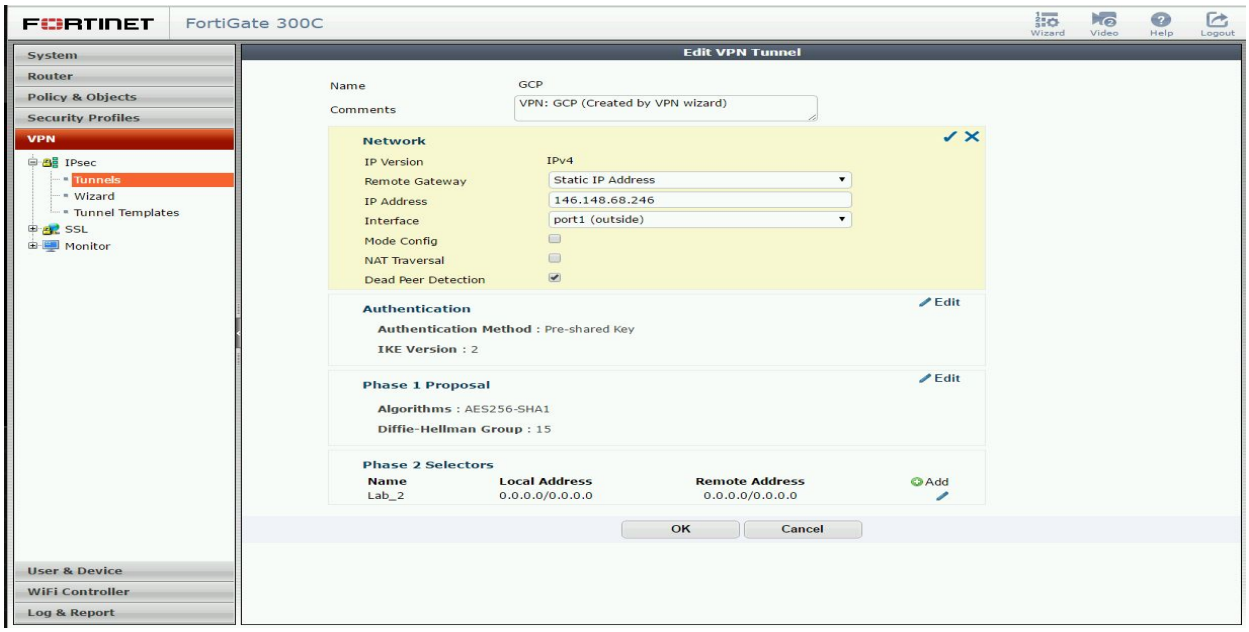
Populate the VPN Tunnel configuration **Network** section as pictured below:

Remote Gateway: select “Static IP Address”

IP Address: enter the IP address of the Google Cloud VPN Gateway

Interface: select the **public** interface of the Fortinet device

Dead Peer Detection: select this checkbox to enable DPD

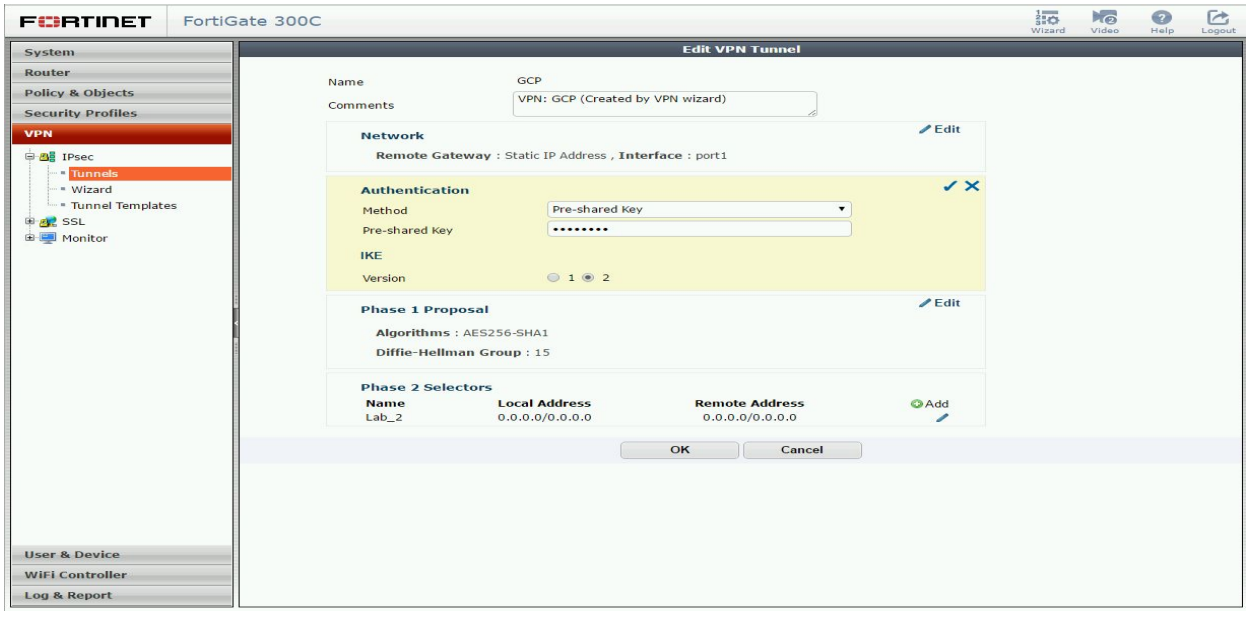


Populate the VPN Tunnel configuration **Authentication** section as pictured below:

Method: for the authentication method select “Pre-Shared Key”

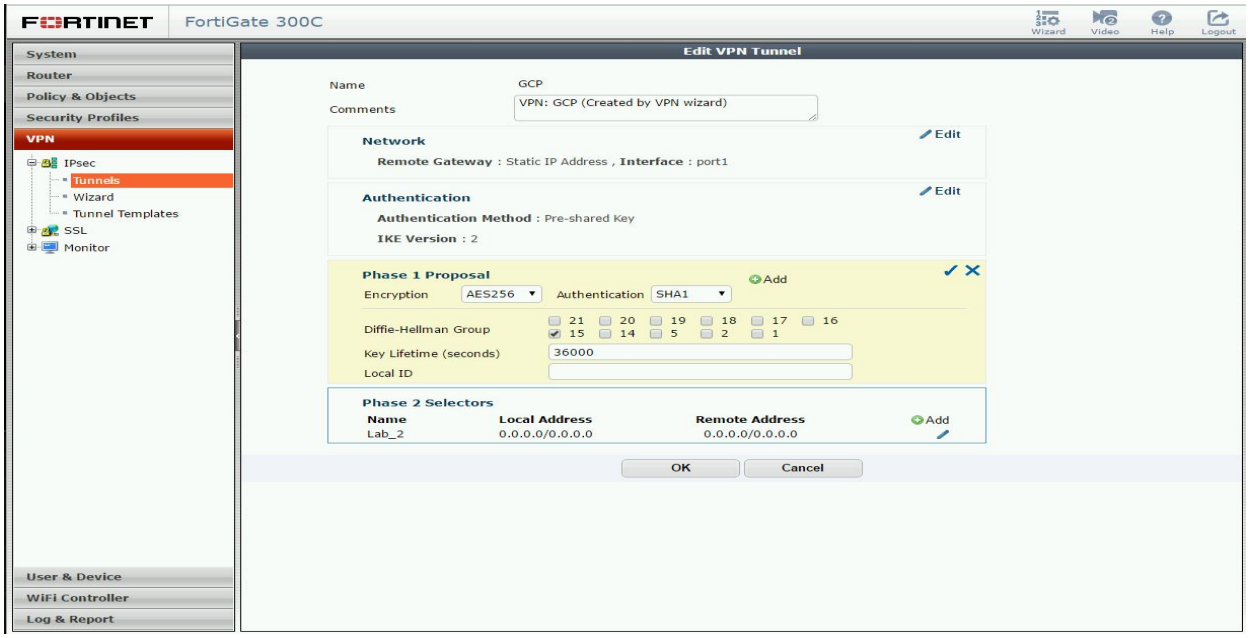
Pre-Shared-Key: enter the pre-shared key you have chosen to use

IKE: select IKE version 2

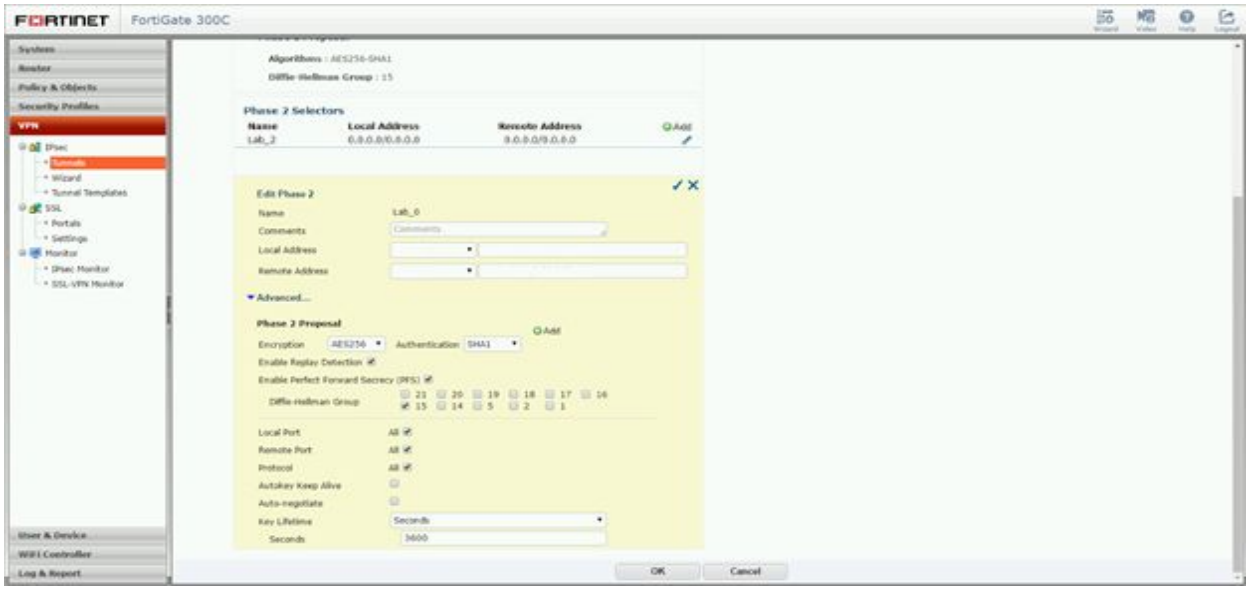


Populate the VPN Tunnel configuration **Phase 1 and 2 Proposal** sections as pictured below. Encryption parameters tested for this guide are as follows:

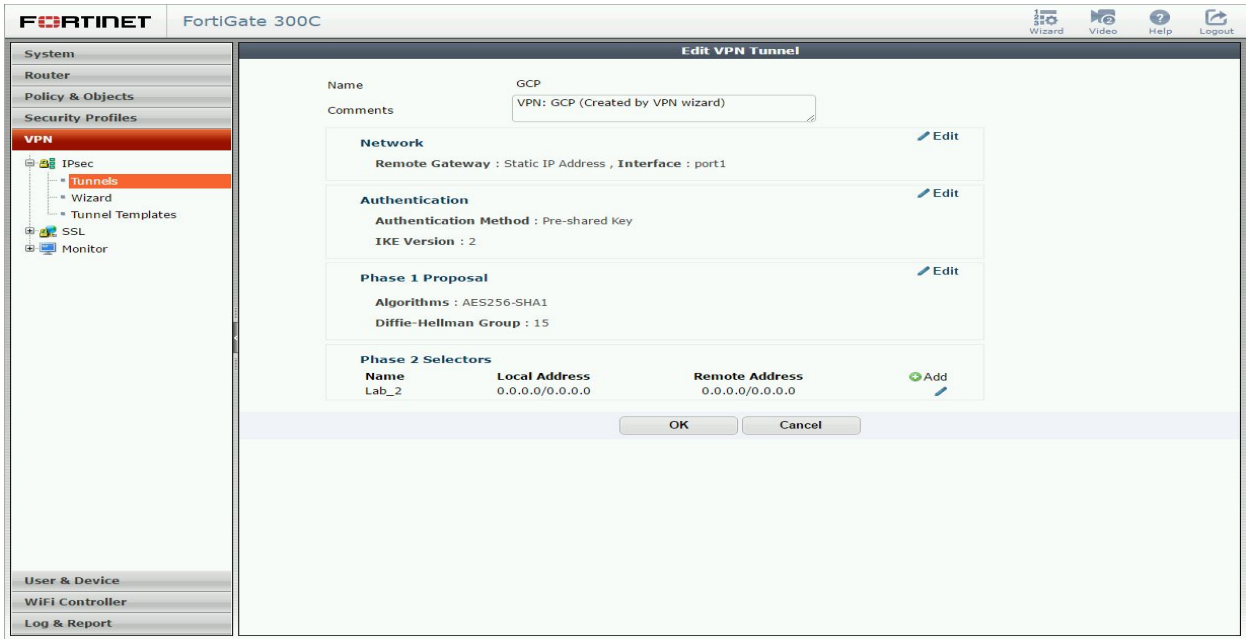
- **Diffe-Hellman Group:** 15
- **Encryption:** AES256
- **Authentication:** SHA1
- **Key Lifetime (Phase 1):** 36000 seconds
- **Key Lifetime (Phase 2):** 10800 seconds
- **Perfect Forward Secrecy:** Enabled



Populate the VPN Tunnel configuration **Phase 2 Proposal** section as pictured below. Note that for the BGP configuration, only one traffic selector needs to be configured with both **Local Address** and **Remote Address** set to 0.0.0.0/0.0.0.0. BGP will handle route distribution for any subnets on either side of the tunnel defined by the BGP policy:

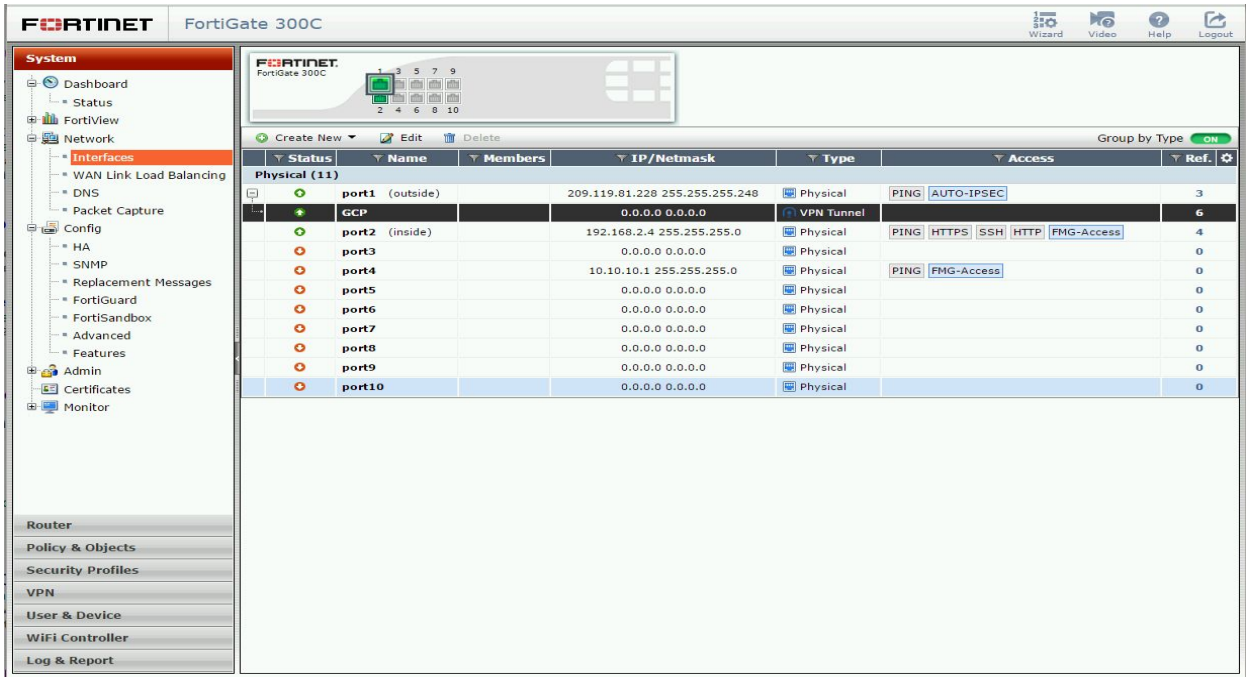


The completed tunnel configuration will appear as shown below:

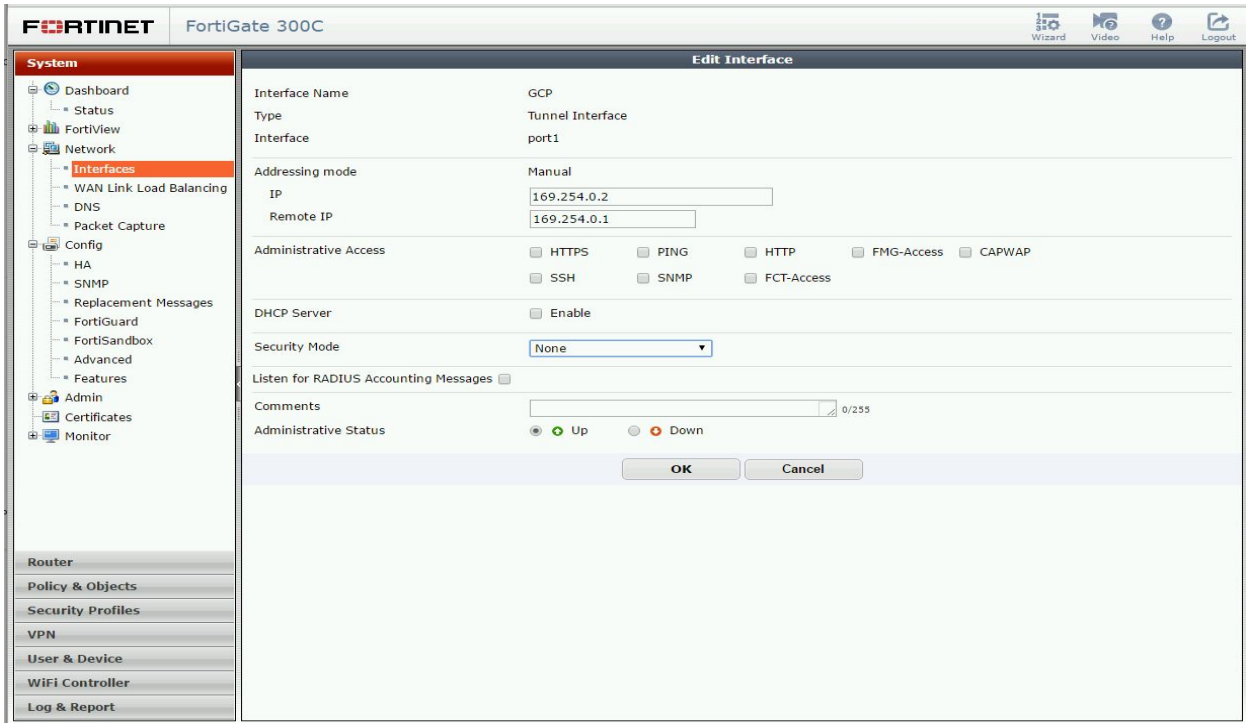


Tunnel Interface

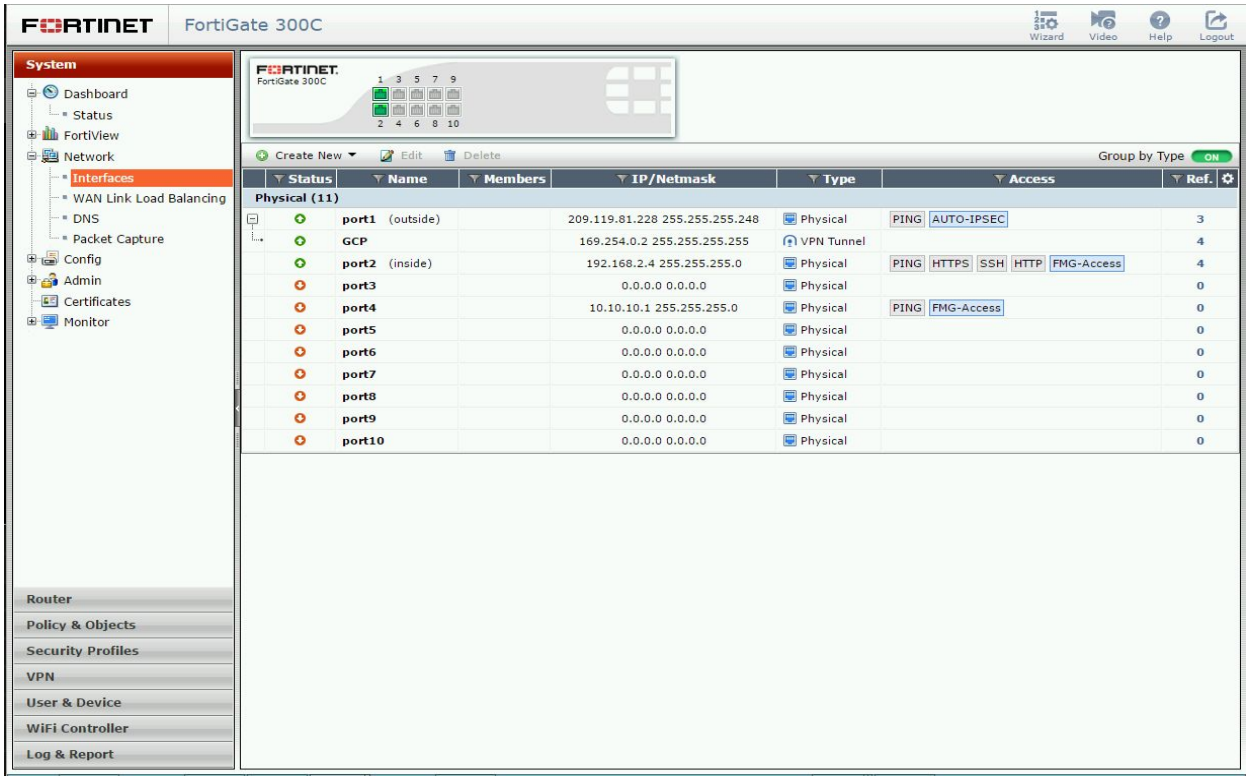
The VPN Wizard used in the IPsec Configuration section will automatically create a virtual tunnel interface which will be used as the IPsec tunnel endpoint. This interface will not have an IP address, however, and the Wizard will not prompt for one. For the BGP configuration, the virtual tunnel inside must be addressed as the BGP peer. Multi-hop BGP is not supported. To add an IP address to the tunnel interface, select **Network** and **Interface** from the sidebar menu. Locate the VPN tunnel entry created by the VPN Wizard and click **Edit**:



The **Edit Interface** UI allows the **IP** and **Remote IP** for the tunnel interface to be set. The IP should be set to the BGP peer address allocated to the remote location in the Google Cloud Router VPN Tunnel configuration section and the Remote IP should be set to the address allocated to the Google Cloud Router. After entering the appropriate IP info, click **OK**:



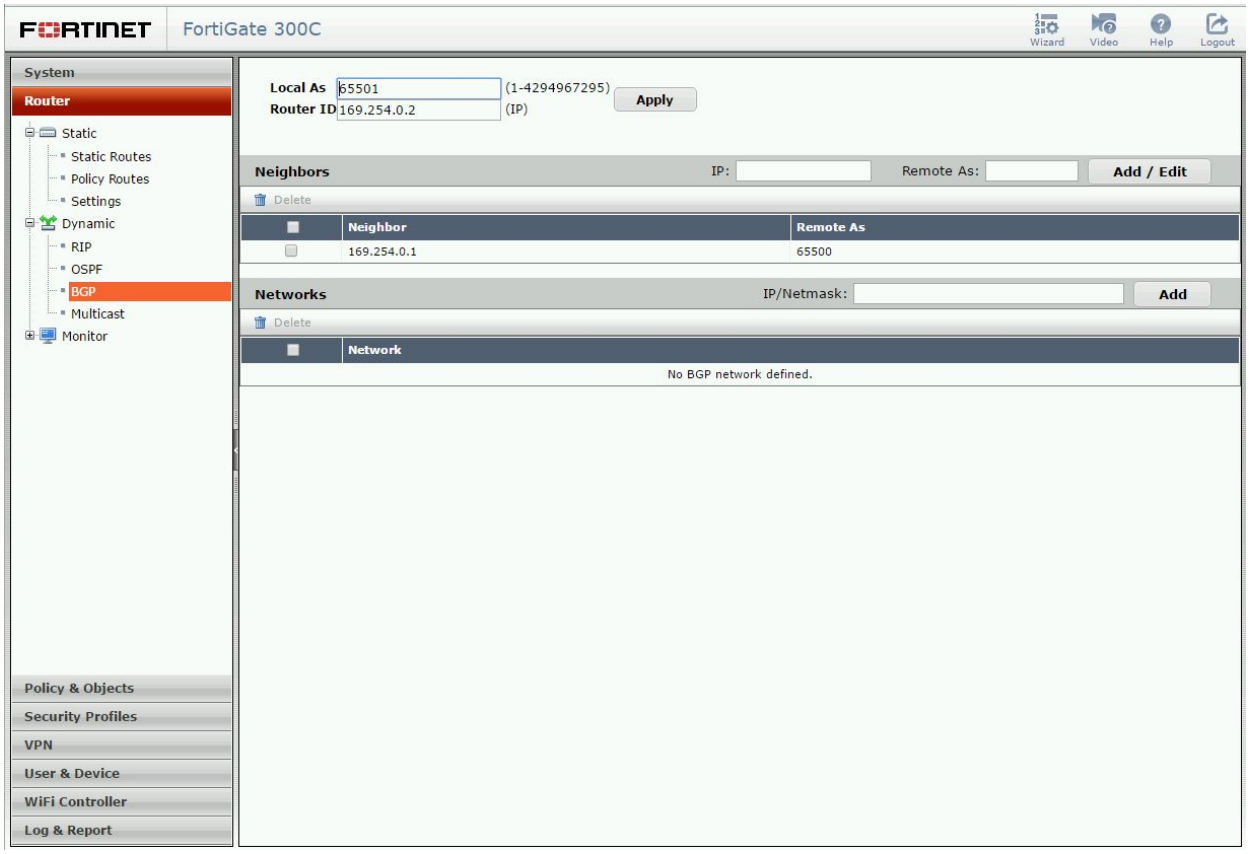
The VPN Tunnel interface should display the configured IP address:



BGP

The final step is to configure BGP routing. From the **Routing** section in the sidebar menu, select **Dynamic**, then **BGP**. Local and neighbor BGP info must be entered to complete the BGP configuration. BGP parameters set in the Google Cloud Router configuration section are used here:

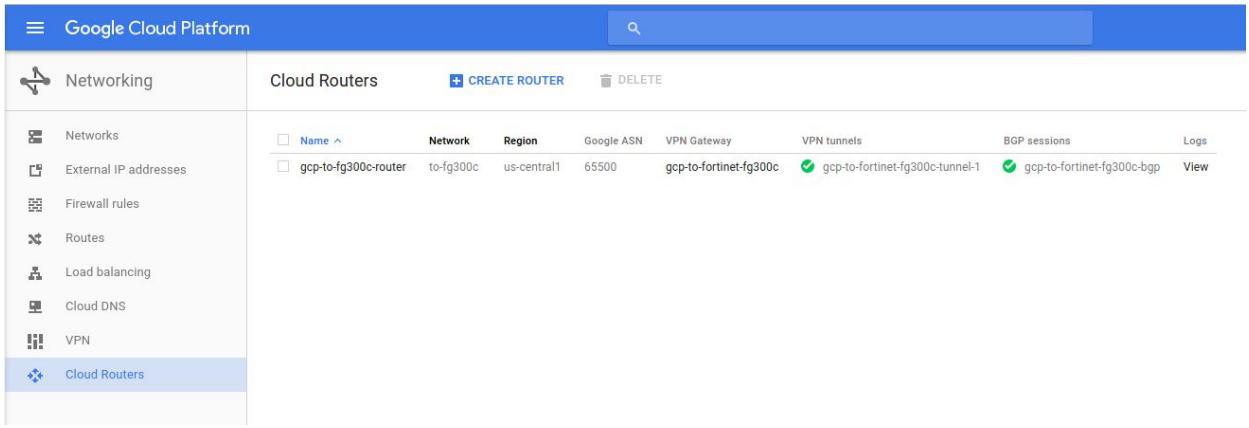
- **Local AS**: the Autonomous System number set for the **remote peer**
- **Router ID**: the IP address set for the **remote peer**
- **Neighbor IP**: the IP address set for the **Google Cloud Router**
- **Remote AS**: the Autonomous System number set for the **Google Cloud Router**



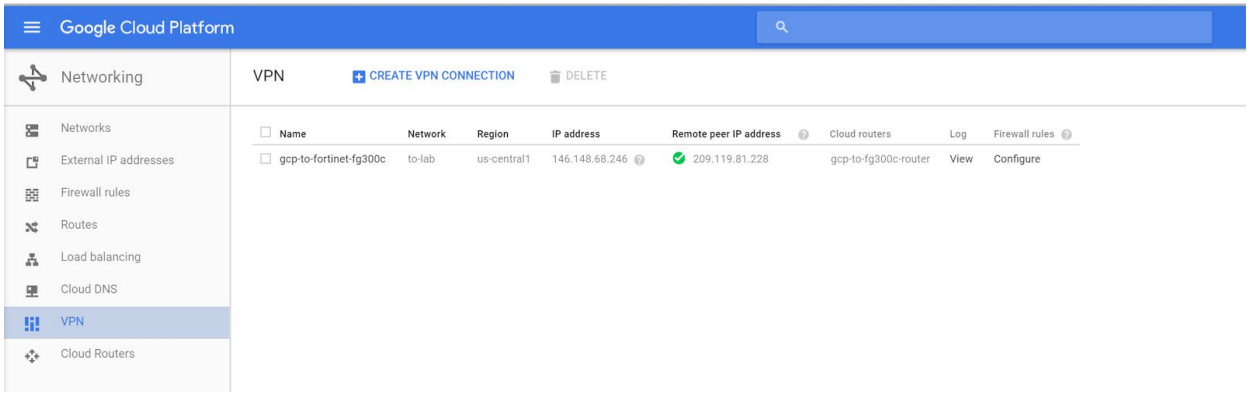
Testing the Site-to-Site VPN

Verify Connectivity

To verify that Cloud Router has successfully initiated BGP peering with AWS, check the Cloud Router status in the Developer Console:



To verify that the IPsec tunnel has been successfully initiated, check the VPN status in the Developer Console:



Testing the Tunnel

Basic Ping

To test the IPsec tunnel traffic selectors, ping a host on each subnet specified in the tunnel configuration from a host attached to the Google Cloud Platform network: